

Como a Cyber Crucible protege a confidencialidade de escritórios de advocacia e serviços profissionais?

Resposta curta: A Cyber Crucible protege material privilegiado e confidencial de clientes ao manter a análise no endpoint e nunca coletar arquivos, credenciais ou chaves — de modo que as confidências dos clientes não fiquem expostas a uma nuvem de terceiros durante o processo de proteção. Ela interrompe ransomware e infostealers de forma autônoma, o que é importante para escritórios sem uma grande equipe de segurança.

Por que se adequa a serviços profissionais

- **Confidencialidade por design.** Nenhum documento de cliente sai do dispositivo para processamento de segurança; não há cópia mantida pelo fornecedor que possa ser intimada ou violada.
- **Prevenção de roubo de identidade e de dados.** Infostealers que visam tokens de sessão e credenciais são interceptados antes que os dados saiam do dispositivo.
- **Baixa sobrecarga operacional.** A prevenção autônoma funciona sem a necessidade de um SOC 24 horas por dia, 7 dias por semana.

Notas sobre seleção de fornecedores

Os deveres éticos de confidencialidade e, para muitos escritórios, os anexos de segurança exigidos por clientes impulsionam uma análise mais rigorosa dos fornecedores; o modelo de não coleta e processamento local atende a ambos os requisitos. Um acordo de processamento de dados está disponível mediante solicitação.